



STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

290 - REMOVAL OF PROHIBITED FOREIGN PRODUCTS STANDARD

Purpose

Pursuant to Governor Evers' Executive Order #184, the Removal of Prohibited Foreign Products Standard is intended to provide standardization on the removal of prohibited foreign products and technologies from State of Wisconsin IT Systems. This standard applies to all State of Wisconsin Executive Branch agencies; where statutorily authorized under subchapter VII of Chapter 16 but excluding the Board of Regents of the University of Wisconsin System. Executive Branch Agencies are to develop policies, procedures, or processes for their own State information and systems to protect State information, where applicable. Non-executive branch agencies are also strongly encouraged to adopt and adhere to this standard.

Standard

The Wisconsin Department of Administration (DOA) Division of Enterprise Technology (DET) is responsible for establishing, and has already established, security and safeguards for State information and information systems (Wis. Stat. §§ 16.971-16.975). DOA-DET is led by the State Chief Information Officer (State CIO) and State Chief Information Security Officer (State CISO) who continually monitor cybersecurity and implement all feasible technical means to ensure the security of all State information and information systems.

Using information gathered through state, federal, and industry-led intelligence, certain vendors and products currently present an unacceptable level of cybersecurity risk to the State, including products and applications where the State has a reasonable belief that the manufacturer or vendor may participate in activities such as but not limited to:

- Collecting sensitive citizen, financial, proprietary, intellectual property, or other business data;
- Enabling email compromise and acting as a vector for ransomware deployment;
- Conducting cyber-espionage against government entities;
- Conducting surveillance and tracking of individual users; and
- Using algorithmic modifications to conduct disinformation or misinformation campaigns.

Pursuant to Governor Evers' Executive Order #184 and Wis. Stat. §§ 16.971-16.975, DOA-DET will continue to use information gathered through state, federal, and industry-led intelligence to investigate vulnerabilities presented by products from foreign vendors. If the State CISO determines that there are security vulnerabilities or deficiencies in any State information systems, the State CISO may determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.



STATE OF WISCONSIN

DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

Products Subject to this Standard:

Given that technology rapidly evolves and changes, it is not feasible to provide a complete list of prohibited products in this standard. In collaboration with the Governor, the Office of the Governor, and state, federal, and industry-led intelligence, DOA-DET will continue to evaluate and identify applications and vendors, due to the risk presented to state information or state information systems, may not be used in, or connected to any State network or installed on any State-issued device, including but not limited to desktop computers, laptops, tablets, cellular phones and other mobile devices.

The State CISO shall communicate any identified prohibited foreign products to the Wisconsin Information Sharing and Analysis Committee (WI ISAC) and Agency IT Directors, per DET's normal communications processes.

As of 1/12/2023, the following vendors and/or software are prohibited from being utilized:

- TikTok
- Huawei Technologies
- ZTE Corp
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- Tencent Holdings, including but not limited to:
 - Tencent QQ
 - QQ Wallet
 - WeChat
- Alibaba products, including but not limited to:
 - AliPay
- Kaspersky Lab

Required Actions:

DOA-DET shall monitor adherence to this standard and assist impacted Executive Branch agencies to ensure they are able to comply with this standard. DOA/DET, the State CIO and State CISO shall provide support including, but not limited to:

- Developing and implementing a plan to remove any prohibited hardware products from State networks;
- Removing any prohibited software products State networks;
- Implementing measures to prevent the installation of prohibited hardware and software products on State-owned, State-leased, or State-managed technology assets;
- Implementing network-based restrictions to prevent the use of, or access to, prohibited services; and
- Incorporating the risks associated with these technologies into security awareness training.



STATE OF WISCONSIN

DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

Definitions

Executive Branch Agency – Has the meaning given under subchapter VII of Chapter 16 but excludes the University of Wisconsin System pursuant to Wis.Stat.Sec. 16.971(2)(j).

State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the agency.

Information Asset – All State information and State information systems and environments.

Compliance References

[240 System and Services Acquisition Standard Executive Branch.pdf \(wi.gov\)](#)

[280 Supply Chain Risk Management.pdf \(wi.gov\)](#)

[Official Website for Wisconsin Governor Tony Evers Executive Orders](#)

[Wisconsin Legislature: 16.754](#)

[Policy Network | Acquisition.GOV](#)

Exception Process

Exceptions to any Executive Branch Agency's Security Policies Standards must follow the Executive Branch Risk Exception Procedure.

Document History and Ownership

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until revised, updated, or retired.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.



STATE OF WISCONSIN

DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
 Kathy Blumenfeld, Secretary
 Trina Zanow, Division Administrator
 Effective Date: 08/01/2023

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	01/12/2023		Reviewer: DOA/DET CIO, Deputy CIO and State CISO Author: DOA/DET Deputy CISO	01/12/2023
2.0	02/20/2023	Revisions to definition of Executive Branch Agency	Reviewer: DOA/DET CIO, Deputy CIO and State CISO Author: DOA/DET Deputy CISO	02/20/2023
3.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/Enterprise IT Author: DOA/DET/BOS	08/01/2023
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and Approved by:

Trina Zanow, CIO

DocuSigned by:

Trina Zanow
 Signature

8/1/2023 | 1:49 PM CDT

Print/Type
 Title

Date